

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA
CHARLESTON

IN THE MATTER OF THE SEARCH OF:

Content of files submitted CASE NO. 2:23-mj-00105
In connection with Cyber Tipline
Reports #133973799 and #133989439,
currently in the custody of
Homeland Security Investigations,
and more fully described in
Attachment A.

AFFIDAVIT

Your Affiant, Andrew C. Hayden, having been duly sworn, does hereby depose and state that the following is true to the best of my information, knowledge, and belief:

I. INTRODUCTION

1. I am a Special Agent with Homeland Security Investigations ("HSI") and have been so employed since 2017. I am a graduate of the Criminal Investigations Training Program and the Immigration and Customs Enforcement ("ICE"), HSI Special Agent Training Program at the Federal Law Enforcement Training Center at Glynco, Georgia. Prior to HSI, I was the Chief Criminal Investigator for the Missouri Bureau of Narcotics and Dangerous Drugs and a Criminal Investigator for the Missouri Department of Corrections. I have a master's degree in Homeland Security with a primary emphasis in Criminal Justice. My duties as an agent for HSI include, but

are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21 and 31 of the United States Code.

2. As part of my duties as an HSI Special Agent, I investigate criminal violations relating to child exploitation and child pornography (hereinafter referred to as "child sexual abuse material" or "CSAM") including violations pertaining to the illegal production, distribution, receipt, and possession of CSAM material, in violation of 18 U.S.C. §§ 2251 and 2252A and as defined by 18 U.S.C § 2256. I have received training in the area of CSAM and have had the opportunity to observe and review examples of CSAM material (as defined by 18 U.S.C. § 2256) in all forms of media including electronic media. I have participated in multiple enforcement operations which have involved CSAM-related offenses.

3. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property-file(s) submitted in connection with Cyber Tipline Reports #133973799 and #133989439 ("the CyberTips"), which are currently in the possession of law enforcement. The files submitted in connection with the CyberTips (more fully described in Attachment A), and the data located therein, there being probable cause to believe that located in the

place described in Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and § 2252A(a)(1), the transportation of child pornography in interstate commerce.

4. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(1), transportation of child pornography in interstate commerce; 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and 2252A(a)(5)(B), possession of child pornography; and are located in the place described in Attachment A.

5. The information contained within the Affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

II. RELEVANT STATUTES

6. The investigation concerns potential violations of 18 U.S.C. §§ 2252A(a)(1), (2), and (5)(B), relating to

matters involving the sexual exploitation of minors.

- a. 18 U.S.C. 2252A(a)(1) prohibits any person from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.
- b. 18 U.S.C. § 2252A(a)(2) prohibits any person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.
- c. 18 U.S.C § 2252A(a)(5)(B) prohibits any person from knowingly possessing any books, magazines, periodicals, films, video tapes, computer discs or other matter that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means including computer, or that was produced using materials mailed, shipped, or transported in interstate or foreign commerce by any means including computer.

III. DEFINITIONS

7. The following terms are relevant to this Affidavit in support of this application for a search warrant:

- a. Child Erotica: The term "child erotica" means any

material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.

- b. Child Pornography: The term "child pornography" is defined at 18 U.S.C. § 2256(8). It consists of a visual depiction of sexually explicit conduct where
 - (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct,
 - (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or
 - (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct, as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. See 18 U.S.C. §§ 2252 and 2256(2), (8).
- c. Internet Protocol ("IP") Address: An "IP address" is a unique number used by a computer or other digital device to access the Internet. Every

computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

- d. Minor: The term "minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- e. Sexually Explicit Conduct: The term "sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic

area of any persons. See 18 U.S.C. § 2256(2).

f. Visual Depictions: "Visual depictions" include undeveloped film and videotape, and data stored on computer disc or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

IV. CYBERTIPLINE REPORT AND PROBABLE CAUSE

8. The National Center for Missing and Exploited Children ("NCMEC") is an organization that, among other things, tracks missing and exploited children, and serves as a repository for information about child pornography.

9. Companies that suspect child pornography has been stored or transmitted on their systems can report that information to NCMEC in a CyberTip. To make such a report, a company providing services on the internet, known as an electronic service provider ("ESP"), can go to an online portal that NCMEC has set up for the submission of these tips. The ESP, in this case Google, can then provide to NCMEC information about the child exploitation activity it believes has occurred, including the incident type, the incident time, any screen or usernames associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. Other than the incident type and

incident time, the remainder of the information the ESP provides is voluntary and undertaken at the initiative of the reporting ESP. The ESP may also upload to NCMEC any files it collected in connection with the activity. The ESP may or may not independently view the content of the files it uploads.

10. NCMEC does not review the content of these uploaded files not previously viewed by the ESP. Using publicly available search tools, NCMEC attempts to locate where the activity occurred based on the information the ESP provides, such as IP addresses. NCMEC packages the information from the ESP along with any additional information it has, such as previous related CyberTips, and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

11. On or about September 9, 2022, electronic service provider Google submitted Cybertip #133973799 to NCMEC. The incident type was identified as apparent child pornography, and the incident time was listed as: September 9, 2022, at 15:55:11 Coordinated Universal Time (UTC).

12. Google also uploaded one file in connection with the report, an alleged media file of apparent child pornography, the content of which NCMEC did not review. The Cybertip indicated that Google did not review the contents of the flagged media file of suspected child pornography:

alphanumeric file "z78_hjfCTGWZ7-Rg.mp4."

13. NCMEC used publicly available search tools to discover that the IP address Google reported resolved to Suddenlink Communications. The CyberTip was then provided to law enforcement in this jurisdiction.

14. I know from my training and experience that hash values are widely used by most ESPs and others, including law enforcement, to identify files. A hash value is akin to a fingerprint for a file. A hash value is obtained by processing the contents of a file through a cryptographic algorithm, which produces a unique numerical value, the hash value, which identifies the unique contents of the file. If the contents of the file are modified in any way, the value of the hash will also change.

15. I know from my training and experience that many ESPs compare the hash values of files that its customers transmit on its systems against a database containing hash values of known child pornography material. If the ESP finds that a hash value on its system matches one in the database, the ESP captures the file along with information about the user who uploaded, posted, possessed, or otherwise transmitted the file on the ESP's systems. This information is then transmitted to NCMEC in the form of a Cybertip.

16. The image file at issue here, alphanumeric file

"z78_hjfCTGWZ7-Rg.mp4," was flagged by the ESP based on a hash match.

17. Based on information contained in the Cybertip, it appears that Google did not independently review any of the material submitted in connection with the Cybertip. Although Google did not review this material, I have probable cause to believe the material contains child pornography, by virtue of the hash match to a database of known child pornography. The Cybertip categorized the image file as a pubescent minor engaged in a sex act.

18. On or about September 10, 2022, Google submitted Cybertip #133989439 to NCMEC. The incident type was identified as apparent child pornography, and the incident time was listed as: September 10, 2022, at 04:33:17 UTC.

19. Google also uploaded one file in connection with the report, a media file of apparent child pornography, the content of which NCMEC did not review. The Cybertip indicated that Google did not review the contents of the flagged media file of suspected child pornography: alphanumeric file "<https://t.co/I4jzuUdOWR.mp4>."

20. NCMEC used publicly available search tools to discover that the IP address the ESP reported resolved to Suddenlink Communications. The Cybertip was then provided to law enforcement in this jurisdiction.

21. The image file at issue here, alphanumeric file "https_t.co_I4jzuUdOWR.mpy," was flagged by the ESP based on a hash match.

22. Based on information contained in the Cybertip, it appears that Google did not independently review any of the material submitted in connection with the Cybertip. Although Google did not review this material, I have probable cause to believe the material contains child pornography, by virtue of the hash match to a database of known child pornography. The Cybertip categorized the image file as a pubescent minor engaged in "lascivious exhibition".

23. In or about October 2022, another agent at HSI was working on this investigation and inadvertently viewed the files attached to the Cybertips outlined above.¹ Once he determined that these two files had not been viewed by Google, he immediately flagged the issue. Your Affiant then took over the investigation and now makes application for this search warrant.

24. In summary, there is probable cause to believe that the material in the files "z78_hjfCTGWZ7-Rg.mp4" and

¹ Accessing these files was not deliberate. The agent sought and obtained search warrants to access files submitted with several other Cybertips linked to this investigation that had not been viewed by the ESP, but unintentionally missed the need for a search warrant for the two Cybertips referenced in Attachment A.

"<https://t.co/I4jzuUdOWR.mp4>" that Google sent to NCMEC in connection with the Cybertips contain child pornography, including any material that may not have been previously reviewed by Google.

II. INTERSTATE NEXUS

25. I submit that the element of "in or affecting interstate or foreign commerce" is satisfied for a violation of 18 U.S.C. § 2252A, for the limited purpose of securing a search warrant, through use of the ESP servers and use of the Internet in connection with this offense.

VI. CONCLUSION

26. Based on the aforementioned factual information, your Affiant respectfully submits that there is probable cause to believe that inside the files that Google uploaded in connection with the above Cybertips #130902706 and #133989439 (described in Attachment A), will be found evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(1), transportation of child pornography; 18 U.S.C. § 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and 18 U.S.C. § 2252A(a)(5)(B), possession of child pornography (described in Attachment B) will be found.

27. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and

seizure of the items described in Attachment A, for the items listed in Attachment B.

I swear that this information is true and correct to the best of my knowledge.

Andrew C. Hayden
SPECIAL AGENT ANDREW C. HAYDEN
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

SUBSCRIBED and SWORN to before me by telephonic means this 23rd day of May, 2023.

Dwane L. Tinsley
DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE